Javier L. Merino
Marc E. Dann (*pro hac vice anticipated*)
Brian D. Flick (*pro hac vice anticipated*)
THE DANN LAW FIRM, PC
372 Kinderkamack Road, Suite 5
Westwood, NJ 07675
Phone: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

Additional counsel listed in signature block below

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

THOMAS SAUNDERS, individually and on behalf of all others similarly situated, Plaintiff, vs. **COLLABERA INC.** Defendant.	Civil Action No. **CLASS ACTION COMPLAINT FOR DAMAGES** **JURY DEMAND ENDORSED HEREON**

Plaintiff THOMAS SAUNDERS ("Plaintiff"), by and through his attorneys, brings this Class Action Complaint on behalf of himself, and all other persons similarly situated, against Defendant COLLABERA INC. ("Collabera" or "Defendant"). All allegations made in this Complaint are made based on information and belief and investigation of counsel, except those allegations that pertain to Plaintiff, which are based on personal knowledge. Each allegation in this Complaint has evidentiary support, or alternatively, pursuant to Rule 11(b)(3) of the Federal Rules of Civil Procedure, is likely to have evidentiary support after a reasonable opportunity for further investigation or discovery.

INTRODUCTION

1. Collabera is a corporate staffing company with offices around the world.[1]

2. Collabera maintains personally identifiable information ("PII") relative to workers' names, addresses, telephone numbers, social security numbers ("SSN"), dates of birth, employee benefits and employee verification information, passport/visa information, and e-mail addresses.[2]

3. On July 10, 2020, Collabera sent correspondence captioned Notice of Data Breach ("Notice") to Plaintiff and all potentially affected employees, a copy of which is attached hereto as Exhibit 1.

4. The Notice notified Plaintiff and all other potentially affected employees that Collabera identified malware on June 8, 2020 in its network system consistent with a ransomware attack. *See* Exhibit 1, p. 1.

5. The Notice notified Plaintiff and all other potentially affected employees that on June 10, 2020 Collabera confirmed that an unauthorized third party obtained its employees' personal and financial information from its network system, including first and last names, mailing addresses, telephone numbers, SSNs, dates of birth, employee benefits and employee verification information, passport/visa information, and e-mail addresses (the "Data Breach"). *See* Exhibit 1, p. 1.

6. At the time of the Data Breach, it is not known how many records were in Collabera's database but upon information and belief the database contained more than 16,000 employee's PII records.[3]

---

[1] https://www.collabera.com/about/company/

[2] Shaun Nichols, *Collabera hacked: IT staffing'n'services giant hit by ransomware, employee personal data stolen*, July 14, 2020 at https://www.theregister.com/2020/07/14/collabera_ransomware/; *see also* Exhibit 1

[3] https://www.collabera.com/about/company/

7. On information and belief, Defendant failed to adopt, implement, maintain, and enforce proper data security policies and procedures which resulted in Plaintiff's and other similarly situated individuals' PII being improperly disclosed to unauthorized third parties. As a result, Plaintiff and the Class members have been injured through the loss of control of their PII, the need to spend time to take appropriate steps to mitigate their injury, and the heightened and imminent risk of identity theft or fraud.

8. Plaintiff brings this suit on behalf of himself and a Class of similarly situated individuals against Defendant for Defendant's failure to protect their PII.

PARTIES

9. Plaintiff Thomas Saunders is a natural person and resident and citizen of Cuyahoga County, Ohio.

10. Defendant Collabera Inc. is a Delaware Corporation with a principal place of business located at 110 Allen Road, Basking Ridge, NJ 07920.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Defendant because it regularly conducts business in New Jersey, and has its headquarters in New Jersey.

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because Plaintiff believes the amount in controversy in this matter exceeds $5,000,000 and because members of the putative Class are from different states than Defendant. Indeed, according to a recent news article, Defendant's database contained records for at least "tens of thousands" of individuals.[4]

[4] Shaun Nichols, *Collabera hacked: IT staffing'n'services giant hit by ransomware, employee personal data stolen*, July 14, 2020 at https://www.theregister.com/2020/07/14/collabera_ransomware/

13. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(2), because a substantial portion of the transactions and occurrences relevant to this action took place in this District. Venue is also proper in this District, pursuant to 28 U.S.C. § 1391(b)(1) as Collabera is subject to this District's personal jurisdiction

DAMAGES FROM DATA BREACHES

The Value of Personal Identifying Information

14. It is well known that PII, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

15. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[5]

16. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[6]

17. Consumers are particularly concerned with protecting the privacy of their financial account information and SSNs, which are the "secret sauce" that is "as good as your DNA to hackers."[7] There are long-term consequences to data breach victims whose SSNs are taken and used by hackers. Even if they know their SSNs have been accessed, Plaintiff and Class members cannot obtain new SSNs unless they become a victim of SSN misuse. Even then, the Social

[5] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

[6] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf

[7] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html

Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[8]

18. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

19. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if they learn someone has abused their information), reviewing their credit reports, contacting companies to dispute fraudulent charges on accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

20. Identity thieves use another's personal information, such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

21. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's photograph; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

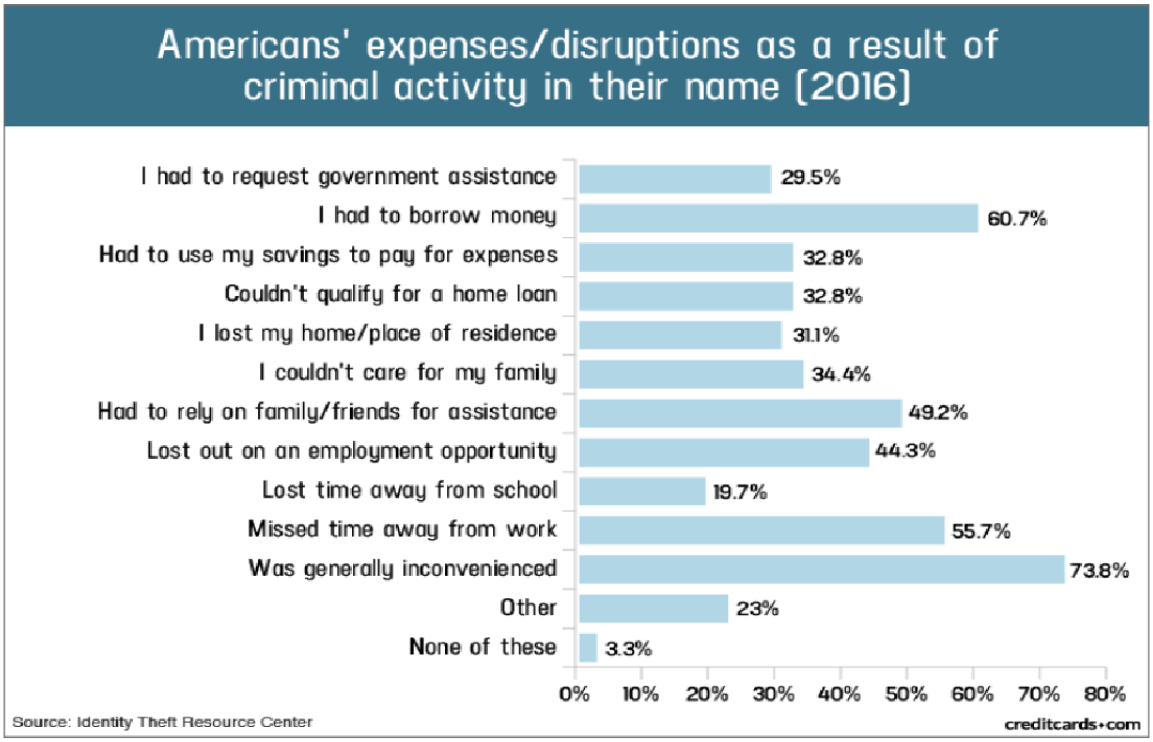
---

[8] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf

[9] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (the "GAO Report")

[10] *See* https://www.identitytheft.gov/Steps

22. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

23. There may be a time lag between when harm occurs and when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

24. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

25. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

Industry Standards for Data Security

26. Data breaches are preventable.[11] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[12] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[13]

27. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[14]

28. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, and Equifax, Defendant is, or reasonably should have been, aware

[11] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012)
[12] *Id.* at 17
[13] *Id.* at 28
[14] *Id.*

of the importance of safeguarding its customers' PII, as well as of the foreseeable consequences of its systems being breached.

29. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

A. Maintaining a secure firewall configuration;

B. Monitoring for suspicious or irregular traffic to servers;

C. Monitoring for suspicious credentials used to access servers;

D. Monitoring for suspicious or irregular activity by known users;

E. Monitoring for suspicious or unknown users;

F. Monitoring for suspicious or irregular server requests;

G. Monitoring for server requests for PII;

H. Monitoring for server requests from VPNs; and

I. Monitoring for server requests from Tor exit nodes.

30. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[15] and protection of PII[16] which includes basic security standards applicable to all types of businesses.

31. The FTC recommends that businesses:

A. Identify all connections to the computers where you store sensitive information;

B. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

C. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

[15] Start with Security: A Guide for Business, F.T.C. (June 2015), https://www.ftc.gov/system/files/ documents/plain-language/pdf0205-startwithsecurity.pdf

[16] Protecting Personal Information: A Guide for Business, F.T.C. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf

D. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

E. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

F. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

G. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

H. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day;

I. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

32. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet

their data security obligations.[17]

33. Because Defendant was entrusted with its employees' PII, it had, and has, a duty to them to keep their PII secure.

34. Employees, such as Plaintiff and Class members, reasonably expect that when they provide PII to a company, the company will safeguard their PII.

35. Nonetheless, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

THE DATA BREACH

36. Plaintiff and Class members entrusted their PII with Collabera in connection with the employment placement services provided to them by Collabera.

37. On information and belief Collabera exercised significant control and authority over the security of its database containing Plaintiff's and Class members' PII.

38. As set forth above, although the database contained sensitive PII, Defendant failed to implement and adopt reasonable procedures to ensure that Plaintiff's and Class members' PII would be protected from access by malicious third parties. The database contained a security flaw that permitted anyone to access Plaintiff's and Class members' PII.

39. On information and belief, third parties did, in fact, access and obtain Plaintiff's and Class members' PII from the database as a direct result of the Data Breach.

40. Defendant failed to prevent the Data Breach because it did not adhere to commonly accepted security standards and failed to detect that its database was subject to a security breach.

[17] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement

41. Defendant's substandard security practices were a direct and proximate cause of the massive Data Breach compromising the PII of tens of thousands of Americans.

42. The aforementioned harms to Plaintiff and Class members was compounded by the fact that, despite becoming aware of the Data Breach on June 8, 2020 and June 10, 2020, Defendant did not send notice to any potentially affected persons until July 10, 2020.

43. Defendant itself acknowledged the imminent harm caused by the Data Breach, as it is offering two years of free credit monitoring to all of its employees. This credit monitoring is insufficient to protect Plaintiff and Class members as there is often a substantial time lag between when harm occurs and when it is discovered.[18] For example, according to a 2017 study, "the amount of fraud committed based on data breach data that is 2-6 years old ha[d] increased by nearly 400% over the last 4 years."[19]

44. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the PII described above.

FACTS RELEVANT TO PLAINTIFF

45. Plaintiff is a citizen of Ohio (and was during the period of the Data Breach).

46. Prior to the Data Breach and during the period of the Data Breach, Plaintiff was employed by Collabera to various third-party placements.

47. On or about July 10, 2020 Plaintiff received the Notice (Exhibit 1) from Collabera.

---

[18] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,*" at 29, U.S. Government Accountability Office, June 2007, *available at* https:/www.gao.gov/new.items/d07737.pdf

[19] Brian Stack, "Here's How Much Your Personal Information is Selling for on the Dark Web," Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web

48. After reviewing the Notice, Plaintiff learned for the first time that his PII had been compromised and Plaintiff was concerned that his identity may have been stolen on at least one, if not multiple, occasions on June 8, 2020 and/or June 10, 2020.

49. After reviewing the Notice, Plaintiff spent time reviewing his credit reports and bank statements.

50. Since the Data Breach, Plaintiff has been inundated with phishing attempts via text messages, telephone calls and emails at his phone number and email address that were taken in the Data Breach. Plaintiff's PII was stolen in the Data Breach and is being misused by the hackers. Plaintiff has spent several hours listening to the voicemails and reviewing the emails to verify their illegitimacy.

51. As a direct result of the Data Breach, Plaintiff suffered anxiety and emotional distress, and will now have to expend additional time and energy reviewing his financial statements, checking his credit reports, verifying his identity with potential creditors, and monitoring his credit reports.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

52. Plaintiff and Class members have an interest in ensuring that their personal and financial information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

53. In the Notice, Collabera offers limited guidance to Plaintiff and Class members about what to do in the event of a discovery that an account has been compromised. Collabera advises customers to: (a) contact the bank immediately, and (b) change their passwords and

security questions to the accounts.

54. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[20]

55. Plaintiff and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft, and have incurred and will likely incur additional damages in order to prevent and mitigate credit fraud or identity theft. The information exposed in the Data Breach is, by its very nature, the information necessary to apply for and obtain lines of credit and myriad financially-related activities.

56. Plaintiff and Class members have suffered and will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, and damage to their credit, Plaintiff and Class members suffer ascertainable losses in the form of out-of-pocket expenses and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to their accounts;

C. Loss of access to credit as a result of Collabera's unilateral decision to restrict access to these accounts;

D. Purchasing credit monitoring and identity theft prevention;

[20] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf

E. Addressing their inability to withdraw funds linked to compromised accounts;

F. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

G. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

H. Placing freezes and alerts with credit reporting agencies;

I. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

J. Contacting their financial institutions and closing or modifying financial accounts;

K. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

L. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and

M. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

57. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy; they have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft; and they have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, and the diminution in the value and/or use of their PII entrusted to Defendant.

CLASS ALLEGATIONS

58. **Class Definition**: Plaintiff brings this action pursuant to Fed. Civ. R. 23, on behalf of a nationwide class of similarly situated individuals and entities ("the Class"), defined as follows:

> All individuals whose PII was compromised in the Data Breach.
>
> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in

which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

59. **Numerosity**: Upon information and belief, the Class is composed of thousands of Class members, as it was reported that financial and banking documents related to tens of thousands of accounts were affected. Thus, the Class is so numerous that joinder of all members is impracticable. Class members can easily be identified through Defendant's records, or by other means.

60. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiff and Class members, which predominate over any individual issues, including:

A. Whether Defendant adequately protected the personal and financial information of Plaintiff and Class members;

B. Whether Defendant stored the personal and financial information of Plaintiff and Class members without implementing reasonably adequate security to protect the information;

C. Whether Defendant adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the personal and financial information of Plaintiff and Class members;

D. Whether Defendant properly trained and supervised employees to protect the personal and financial information of Plaintiff and Class members;

E. Whether Defendant promptly notified Plaintiff and Class members of the Data Breach;

F. Whether Defendant owed a duty to Plaintiff and Class members to safeguard and protect their personal and financial information;

G. Whether Defendant breached its duty to Plaintiff and Class members to safeguard and protect their personal and financial information;

H. Whether Defendant breached its duty to Plaintiff and Class members by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect their personal and financial information; and

I. Whether Defendant is liable for the damages suffered by Plaintiff and Class members as a result of the Data Breach.

61. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. All claims are based on the same legal and factual issues. Plaintiff and each of the Class members provided their personal and financial information to Collabera, and the information was accessed by unauthorized hackers. Defendant's conduct was uniform with respect to all Class members.

62. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to the Class, and Defendant has no defense unique to Plaintiff.

63. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impractical or impossible for members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiff's claims are manageable.

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

64. Plaintiff repeats and realleges the allegations of paragraphs 1-63 with the same force and effect as though fully set forth herein.

65. Collabera knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiff and Class members and the importance

of adequate security. Collabera was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

66. Collabera had a common law duty to prevent foreseeable harm to those who entrusted their personal and financial information to Collabera. This duty existed because Plaintiff and Class members were foreseeable and probable victims of the failure of Collabera to adopt, implement, and maintain reasonable security measures so that Plaintiff's and Class members' personal and financial information would not be accessible by unauthorized persons.

67. Collabera owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Collabera knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

68. Collabera had a special relationship with Plaintiff and Class members. Collabera was entrusted with Plaintiff's and Class members' personal and financial information, and Collabera was in a position to protect their personal and financial information from unauthorized access and activity.

69. Collabera's duties also arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable

measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of Collabera's duties.

70. Collabera had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' personal and financial information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

71. More specifically, the duties of Collabera included, among other things, the duty to:

A. Adopt, implement, and maintain policies, procedures, and security measures for protecting Plaintiff's and Class members' personal and financial information, including policies, procedures, and security measures;

B. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of Plaintiff's and Class members' personal and financial information with entities that failed to adopt, implement, and maintain policies, procedures, and security measures;

C. Adopt, implement, and maintain reasonable policies and procedures to ensure that Plaintiff's and Class members' personal and financial information is disclosed only with authorized persons who have adopted, implemented, and maintained policies, procedures, and security measures;

D. Properly train its employees to protect documents containing Plaintiff's and Class members' personal and financial information; and

E. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly repel attacks to the security of its systems.

72. Collabera breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' personal and financial information in its possession so that the information would not come within the possession, access, or control of unauthorized persons. The Notice acknowledges that Collabera's database was subject to unauthorized access at least as early as June 8, 2020.

73. Collabera breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized third party access to the Plaintiff's and Class members' PII.

74. Collabera further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII within its possession, custody, and control.

75. Collabera acted with reckless disregard for the security of the personal and financial information of Plaintiff and Class members because Collabera knew or should have known that its data security practices were not adequate to safeguard the personal and financial information that it collected and stored.

76. Collabera acted with reckless disregard for the rights of Plaintiff and Class members by failing to promptly detect the Data Breach and provide prompt notice so that Plaintiff and Class members could take measures to protect themselves from damages caused by the unauthorized access of the accounts compromised in the Data Breach and take measures to ensure the continuity of their financial affairs.

77. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

78. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the Data Breach.

79. The Data Breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

80. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

81. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their PII would not have been compromised.

82. As a result of the conduct of Collabera, Plaintiff and Class members have suffered and will continue to suffer actual damages including, but not limited to, fraudulent transactions on their accounts; expenses and time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

83. Neither Plaintiff nor Class members contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and Class members for the reasonable costs of future credit and identity monitoring services for a reasonable period of time,

substantially in excess of two years. Defendant is also liable to Plaintiff and Class members to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and the Class members have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and Class members to the extent their PII has been diminished in value and that Plaintiff and Class members no longer control that PII and to whom it would be disseminated.

COUNT II
NEGLIGENCE PER SE
(*On behalf of Plaintiff and the Class*)

84. Plaintiff repeats and realleges the allegations of paragraphs 1-63 with the same force and effect as though fully set forth herein.

85. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class members.

86. The FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

87. Defendant solicited, gathered, and stored PII of Plaintiff and the Class members to facilitate transactions which affect commerce.

88. Defendant violated the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII of Plaintiff and the Class members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly

unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

89. Defendant's violation of the FTC Act (and similar state statutes) constitutes negligence per se.

90. Plaintiff and the Class members are within the class of persons that the FTC Act was intended to protect.

91. The harm that occurred as a result of the breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class members.

92. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class members have suffered, and continue to suffer, damages arising from the breach as described above.

COUNT III
INVASION OF PRIVACY
(On behalf of Plaintiff and the Class)

93. Plaintiff repeats and realleges the allegations of paragraphs 1-63 with the same force and effect as though fully set forth herein.

94. Defendant invaded Plaintiff's and the Class members' right to privacy by allowing the unauthorized access to Plaintiff's and Class members' PII and by negligently maintaining the confidentiality of Plaintiff's and Class members' PII, as set forth above.

95. The intrusion was offensive and objectionable to Plaintiff, the Class members, and to a reasonable person of ordinary sensibilities in that Plaintiff's and Class members' PII was disclosed without prior written authorization of Plaintiff and the Class.

96. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class members provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

97. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class members' PII was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class members suffered damages as described herein.

98. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class members' PII with a willful and conscious disregard of Plaintiff's and the Class members' right to privacy.

99. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class members great and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and Class members' PII with sub-standard and insufficient protections.

COUNT IV
INJUNCTIVE RELIEF
(On behalf of Plaintiff and the Class)

100. Plaintiff repeats and realleges the allegations of paragraphs 1-63 with the same force and effect as though fully set forth herein.

101. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and resulting Data Breach have caused (and will continue to cause) Plaintiff and Class members to suffer irreparable harm in the form of, *inter alia*, (i) identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy and PII, (iv) breach of the confidentiality of their PII, (v) deprivation of the value of their PII, for which there is a well-established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

102. Plaintiff and Class members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Defendant to (i) notify each person whose PII was exposed in the Data Breach, (ii) provide credit monitoring to each such person for a reasonable period of time, substantially in excess of two years, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance), and (iv) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and resulting Data Breach.

103. Plaintiff and Class members also are entitled to injunctive relief requiring Defendant to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia,*(i) engaging third party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's computer systems on a periodic basis, (ii) engaging third party security auditors and internal personnel to run automated security

monitoring, (iii) auditing, testing, and training its security personnel regarding any new or modified procedures, (iv) conducting regular database scanning and security checks, (v) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (vi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

104. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury in the event Defendant commits another security lapse, the risk of which is real, immediate, and substantial.

105. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive security lapse, Plaintiff and Class members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Defendant has a pre-existing legal obligation to employ adequate data security measures, Defendant's cost to comply with the above-described injunction it is already required to implement is relatively minimal.

106. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security lapse, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiff, Class members, and the numerous future applicants and employees whose confidential and sensitive PII would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff THOMAS SAUNDERS individually, and on behalf of all others similarly situated, respectfully requests that judgment be entered in his favor against Defendant COLLABERA INC. and for an Order as follows:

A. A finding that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. Appointing Plaintiff as representative of the Class;

C. Appointing Plaintiff's counsel as counsel for the Class;

D. An award of damages for Plaintiff and Class members for all actual damages and all other forms of available relief, as applicable;

E. An award to Plaintiff and Class members of punitive damages and all other forms of available relief, as applicable;

F. An award to Plaintiff and Class members for attorney's fees and costs, including interest thereon as allowed or required by law;

G. An injunction requiring Collabera to adopt, implement, and maintain adequate security measures to protect its employees' personal and financial information, as set forth in Count IV; and

H. Granting all such further and other relief as the Court deems just and appropriate.

Respectfully submitted,

/s/Javier L. Merino
Javier L. Merino
Marc E. Dann (*pro hac vice* anticipated)
Brian Flick (*pro hac anticipated)*
THE DANN LAW FIRM, PC
372 Kinderkamack Road, Suite 5
Westwood, NJ 07675
Phone: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Matthew C. De Re (*pro hac vice* anticipated)
matt@attorneyzim.com
Sharon A. Harris (*pro hac vice* anticipated)
sharon@attorneyzim.com
Jeffrey D. Blake (*pro hac vice* anticipated)
jeff@attorneyzim.com

ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiff and the putative Class

JURY DEMAND

Plaintiff hereby requests a trial by jury on all issues.

/s/Javier L. Merino
Javier L. Merino
THE DANN LAW FIRM, PC